UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/812,651	03/29/2004	Mark D. Yarvis	ITL.1954US (P18388)	3419

47795 7590 08/21/2008

TROP, PRUNER & HU, P.C.
1616 S. VOSS RD., SITE 750
HOUSTON, TX 77057-2631

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
08/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/812,651	**Applicant(s)** YARVIS, MARK D.	
	Examiner KAVEH ABRISHAMKAR	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 June 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,14-20 and 26-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8, 14-20, 26-36* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the Restriction/Election requirement received on June 6, 2008. Claims 1-36 were subject to an election restriction requirement.

Election/Restrictions

2. Applicant's election without traverse of Group I (claims 1-8, 14-20, 26-36) in the reply filed on June 6, 2008 is acknowledged.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3, and 33-36 are rejected under 35 U.S.C. 102(e) as being anticipated by Juels et al. (U.S. Patent Pub. No. US 2006/0033608 A1).

Regarding claim 1, Juels discloses:

An apparatus, comprising:

a detector to determine whether a first radio frequency identification tag read by a reader that reads radio frequency identification tags is a match with a second radio frequency identification tag read by said reader (paragraph 0025-0026, 0067-0068: *compare RFID with identifier*).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Juels discloses:

An apparatus as claimed in claim 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag (paragraph 0025-0026, 0067-0068: *compare RFID with identifier*).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Juels discloses:

An apparatus as claimed in claim 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector authenticates the lock tag when said detector detects the lock tag and the key tag being within a predetermined distance of said detector (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein the RF can only travel predetermined distances*).

Regarding claim 33, Juels discloses:

An apparatus, comprising:

a transceiver to communicate with a radio frequency identification tag (paragraph 0010);

a directional antenna coupled to said transceiver (paragraph 0010); and a detector to determine whether a first radio frequency identification tag read by said transceiver is a match with a second radio frequency identification tag by said transceiver (paragraph 0025-0026, 0067-0068: *compare RFID with identifier*).

Claim 34 is rejected as applied above in rejecting claim 33. Furthermore, Juels discloses:

An apparatus as claimed in claim 33, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag (paragraph 0025-0026, 0067-0068: *compare RFID with identifier*).

Claim 35 is rejected as applied above in rejecting claim 33. Furthermore, Juels discloses:

An apparatus as claimed in claim 33, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector authenticates the lock tag when said detector detects the lock tag and the key tag being within a predetermined distance of said detector (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein the RF can only travel predetermined distances*).

Claim 36 is rejected as applied above in rejecting claim 33. Furthermore, Juels discloses:

An apparatus as claimed in claim 33, wherein said detector determines whether the first radio frequency identification tag is a match with the second radio frequency identification tag or a third or more radio frequency identification tags (paragraph 0025-0026, 0067-0068: *compare RFID with identifier*).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4-8, 14-20, and 26-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Juels et al. (U.S. Patent Pub. No. US 2006/0033608 A1) in view of Lapstun et al. (U.S. Patent 6,789,194).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Juels discloses:

An apparatus as claimed in 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector includes a nonce generator to generate a nonce (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein the RF can only travel predetermined distances*).

Juels does not explicitly disclose encrypting the nonce using a public cryptography key. Lapstun discloses encrypting the nonce and then decrypting the nonce for verification (Lapstun: column 33, lines 45-65). In the system of Juels, the encryption/decryption method of Lapstun can be used to secure the exchange of the nonces. Therefore, it would have been obvious to one of ordinary skill in the art to use the system of Lapstun to encrypt and decrypt the nonces in order to increase the security of the exchanges (Lapstun: column 33, lines 55-57).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Juels discloses:

An apparatus as claimed in claim 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector includes a nonce generator to generate a nonce (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein the RF can only travel predetermined distances*).

Juels does not explicitly disclose encrypting the nonce using a public cryptography key. Lapstun discloses encrypting the nonce and then decrypting the nonce for verification (Lapstun: column 33, lines 45-65). In the system of Juels, the encryption/decryption method of Lapstun can be used to secure the exchange of the nonces. Therefore, it would have been obvious to one of ordinary skill in the art to use the system of Lapstun to encrypt and decrypt the nonces in order to increase the security of the exchanges (Lapstun: column 33, lines 55-57).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Lapstun discloses:

An apparatus as claimed in claim 5, wherein the cryptography key of the lock tag is the same as the cryptography key of the key tag (Lapstun: column 33, lines 45-65).

Claim 7 is rejected as applied above in rejecting claim 5. Furthermore, Lapstun discloses:

An apparatus as claimed in claim 5, wherein the nonce generator generates a series of nonces, wherein the lock tag delays encryption of the nonce with respect to encryption of the nonce by the key tag, and wherein said detector further comprises a delay to delay the encrypted version of the nonce encrypted by the key tag (Lapstun: column 33, lines 45-65).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Juels discloses:

An apparatus as claimed in claim 1, wherein said detector determines whether the first radio frequency identification tag is a match with the second radio frequency identification tag or a third or more radio frequency identification tags (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein the RF can only travel predetermined distances*).

Regarding claim 13, Juels discloses:

A method, comprising:

generating a nonce (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein the RF can only travel predetermined distances*).

Juels does not explicitly disclose encrypting the nonce using a public cryptography key. Lapstun discloses encrypting the nonce and then decrypting the nonce for verification (Lapstun: column 33, lines 45-65). In the system of Juels, the encryption/decryption method of Lapstun can be used to secure the exchange of the nonces. Therefore, it would have been obvious to one of ordinary skill in the art to use the system of Lapstun to encrypt and decrypt the nonces in order to increase the security of the exchanges (Lapstun: column 33, lines 55-57).

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Juels discloses:

A method as claimed in claim 14, further comprising determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein the RF can only travel predetermined distances*).

Claim 16 is rejected as applied above in rejecting claim 14. Furthermore, Lapstun

A method as claimed in claim 14, wherein the cryptography key received from the first radio frequency identification tag is a public key, and wherein the second radio frequency identification tag decrypts the encrypted nonce using a private key associated with the public key (Lapstun: column 33, lines 45-65).

Regarding claim 17, Juels discloses:

A method, comprising:

generating a series of nonces (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein there are multiple RF tags*);

sending the series of nonces to a first radio frequency identification tag and a second radio frequency identification tag (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein there are multiple RF tags*).

Juels does not explicitly disclose encrypting the nonce using a public cryptography key. Lapstun discloses encrypting the nonce and then decrypting the nonce for verification (Lapstun: column 33, lines 45-65). In the system of Juels, the encryption/decryption method of Lapstun can be used to secure the exchange of the nonces. Therefore, it would have been obvious to one of ordinary skill in the art to use the system of Lapstun to encrypt and decrypt the nonces in order to increase the security of the exchanges (Lapstun: column 33, lines 55-57).

Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, Juels discloses:

A method as claimed in claim 17, further comprising determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag (paragraph 0025-0026, 0067-0068: *compare RFID with identifier*).

Claim 19 is rejected as applied above in rejecting claim 17. Furthermore, Lapstun discloses:

A method as claimed in claim 17, wherein the first and second radio frequency identification tags encrypt the series of nonces using the same cryptography key (Lapstun: column 33, lines 45-65).

Claim 20 is rejected as applied above in rejecting claim 17. Furthermore, Lapstun dislcoses:

A method as claimed in claim 17, wherein the first radio frequency radio identification tag delays the series of nonces with respect to the second radio frequency identification tag, and further comprising delaying the encrypted versions of the series of nonces received from the second radio frequency identification tag prior to said comparing (Lapstun: column 33, lines 45-65).

Regarding claim 26, Juels discloses:

An article comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in verification of association of at least two or more radio frequency identification tags by:

generating a nonce (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein there are multiple RF tags*);

sending the nonce to a second radio frequency identification tag (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein there are multiple RF tags*);

receiving the nonce from the second radio frequency identification tag (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein there are multiple RF tags*); and

comparing the nonce generated by said generating to the decrypted nonce (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein there are multiple RF tags*).

Juels does not explicitly disclose encrypting the nonce using a public cryptography key. Lapstun discloses encrypting the nonce and then decrypting the nonce for verification (Lapstun: column 33, lines 45-65). In the system of Juels, the encryption/decryption method of Lapstun can be used to secure the exchange of the nonces. Therefore, it would have been obvious to one of ordinary skill in the art to use the system of Lapstun to encrypt and decrypt the nonces in order to increase the security of the exchanges (Lapstun: column 33, lines 55-57).

Claim 27 is rejected as applied above in rejecting claim 26. Furthermore, Juels discloses:

An article as claimed in claim 26, wherein the instructions, when executed, further result in verification of association of at least two or more radio frequency identification tags by determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag Juels does not explicitly disclose encrypting the nonce using a public cryptography key. Lapstun discloses encrypting the nonce and then decrypting the nonce for verification (Lapstun: column 33, lines 45-65). In the system of Juels, the encryption/decryption method of Lapstun can be used to secure the exchange of the nonces. Therefore, it would have been obvious to one of ordinary skill in the art to use the system of Lapstun to encrypt and decrypt the nonces in order to increase the security of the exchanges (Lapstun: column 33, lines 55-57).

Claim 28 is rejected as applied above in rejecting claim 26. Furthermore, Lapstun discloses:

An article as claimed in claim 26, wherein the cryptography key received from the first radio frequency identification tag is a public key, and wherein the second radio frequency identification tag decrypts the encrypted nonce using a private key associated with the public key (Lapstun: column 33, lines 45-65).

Regarding claim 29, Juels discloses:

An article comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in verification of association of at least two or more radio frequency identification tags by:

generating a series of nonces (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein there are multiple RF tags*);

sending the series of nonces to a first radio frequency identification tag and a second radio frequency identification tag (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein there are multiple RF tags*).

Juels does not explicitly disclose encrypting the nonce using a public cryptography key. Lapstun discloses encrypting the nonce and then decrypting the nonce for verification (Lapstun: column 33, lines 45-65). In the system of Juels, the encryption/decryption method of Lapstun can be used to secure the exchange of the nonces. Therefore, it would have been obvious to one of ordinary skill in the art to use the system of Lapstun to encrypt and decrypt the nonces in order to increase the security of the exchanges (Lapstun: column 33, lines 55-57).

Claim 30 is rejected as applied above in rejecting claim 29. Furthermore, Juels discloses:

An article as claimed in claim 29, wherein the instructions, when executed, further result in verification of association of at least two or more radio frequency identification tags by determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag (paragraph 0025-0026, 0067-0068: *compare RFID with identifier wherein there are multiple RF tags*).

Claim 31 is rejected as applied above in rejecting claim 29. Furthermore, Lapstun discloses:

An article as claimed in claim 29, wherein the first and second radio frequency identification tags encrypt the series of nonces using the same cryptography key (Lapstun: column 33, lines 45-65).

Claim 32 is rejected as applied above in rejecting claim 29. Furthermore, Lapstun discloses:

An article as claimed in claim 29, wherein the first radio frequency radio identification tag delays the series of nonces with respect to the second radio frequency identification tag, and wherein the instructions, when executed, further result in verification of association of at least two or more radio frequency identification tags by comprising delaying the encrypted versions of the series of nonces received from the second radio frequency identification tag prior to said comparing (Lapstun: column 33, lines 45-65).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Examiner, Art Unit 2131

/K. A./
08/19/2008
Examiner, Art Unit 2131